In the Claims:

1.-28. (Cancelled)

29. (Currently Amended) A method of anticipating a device in a networked computer system is to be affected by an anomaly, comprising:

polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communications thereof;

detecting an anomaly ~~at~~ responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and

determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device.

30. (Canceled)

31. (Currently Amended) The method of claim 29, further comprising transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly ~~at the first device~~, the anomaly warning comprising a unique device identifier.

32. (Previously Presented) The method of claim 29, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

33. (Previously Presented) The method of claim 29, wherein detecting the anomaly comprises analyzing a plurality of data packets with respect to predetermined patterns.

34. (Currently Amended) The method of claim 33, wherein analyzing the data packets comprises analyzing data packets that have been received by at least two ~~device~~ devices in the networked computer system.

35. (Currently Amended) The method claim 29, further comprising controlling the second device ~~that is anticipated to be affected by the anomaly~~ responsive to determining the second device is anticipated to be affected by the anomaly.

36-42. (Canceled)

43. (New) The method of Claim 35, wherein controlling the second device responsive to determining the second device is anticipated to be affected by the anomaly comprises controlling a firewall of the second device responsive to determining the second device is anticipated to be affected by the anomaly.

44. (New) The method of Claim 29, wherein determining a second device that is anticipated to be affected by the anomaly is followed by comprising sending an alert to the second device prior to polling of the second device.

45. (New) A computer program product for monitoring a networked computer system, the computer program product comprising computer program code embodied in a storage medium, the computer program code comprising:

program code configured to sequentially poll a plurality of devices of the networked computer system for data relating to network communications thereof;

program code configured to detect an anomaly responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and

program code configured to determine a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers,

and computer sites following the detection of the anomaly and prior to polling of the second device.

46. (New) The computer program product of claim 45, wherein the computer program code further comprises program code configured to transmit an anomaly warning from the first device to a central analysis engine responsive to detecting the anomaly at the first device, the anomaly warning comprising a unique device identifier.

47. (New) The computer program product claim 45, wherein the anomaly comprises one of an intrusion and an intrusion attempt.

48. (New) The computer program product of claim 45, wherein the program code configured to detect an anomaly comprises program code configured to analyze a plurality of data packets with respect to predetermined patterns.

49. (New) The computer program product of claim 48, wherein the program code configured to analyze a plurality of data packets comprises program code configured to analyze data packets that have been received by at least two devices in the networked computer system.

50. (New) The computer program product of claim 45, wherein the computer program code further comprises program code configured to control the second device responsive to determining the second device is anticipated to be affected by the anomaly.

51. (New) The computer program product of claim 50, wherein the program code configured to control the second device responsive to determining the second device is anticipated to be affected by the anomaly comprises program code configured to control a firewall of the second device responsive to determining the second device is anticipated to be affected by the anomaly

52. (New) The computer program product claim 45, wherein the computer program code further comprises program code configured to send an alert to the second device responsive to determining the second device is anticipated to be affected by the anomaly prior to polling of the second device.